

Application No.: 09/872,077
IBM Docket #: STL920000116USI

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Original) A computer system for encrypting and decrypting a data element using a static key and a dynamic key, comprising:
said data element being statically encrypted with said static key;
said data element being dynamically encrypted with said dynamic key; and
said data element being decrypted with said dynamic key and said static key.
2. (Original) The computer system of Claim 1, wherein encryption with said static key is strong encryption.
3. (Original) The computer system of Claim 1, wherein encryption with said dynamic key is weak encryption.
4. (Original) The computer system of Claim 1, wherein:
said data element is encrypted with said static key on a first computer system;
said data element is encrypted with said dynamic key on a second computer system;
said data element is decrypted with said static key and said dynamic key on a third computer system; and
thereby encryption and decryption are distributed between said first computer system, said second computer system, and said third computer system.
5. (Original) The computer system of Claim 4, wherein said second computer system is untrusted.
6. (Original) The computer system of Claim 1, wherein:
said data element is encrypted with said static key on a first computer system;
said data element is encrypted with said dynamic key on said first computer system;
said data element is decrypted with said static key and said dynamic key on a second computer system; and

Application No.: 09/872,077

IBM Docket #: STL920000116US1

thereby encryption and decryption are distributed between said first computer system and said second computer system.

7. (Original) A computer implemented method for encrypting a data element and decrypting said data element using a static key and a dynamic key, comprising:
encrypting said data element with said static key;
encrypting said data element with said dynamic key; and
decrypting said data element with said static key and said dynamic key.
8. (Original) The method of Claim 7 further comprising strongly encrypting said data element with said static key.
9. (Original) The method of Claim 7 further comprising weakly encrypting said data element with said dynamic key.
10. (Original) The method of Claim 7, further comprising:
encrypting said data element with said static key on a first computer system;
transmitting said data element to a second computer system;
encrypting said data element with said dynamic key on said second computer system;
transmitting said data element to a third computer system;
decrypting said data element with said static key and said dynamic key on said third computer system; and
thereby distributing encryption between said first computer system, said second computer system, and said third computer system.
11. (Original) The method of Claim 7, further comprising:
encrypting said data element with said static key on a first computer system;
encrypting said data element with said dynamic key on said first computer system;
transmitting said data element to a second computer system;
decrypting said data element with said static key and said dynamic key on said second computer system; and

Application No.: 09/872,077
IBM Docket #: STL920000116US1

thereby distributing encryption between said first computer system and said second computer system.

12. (Original) The method of Claim 10, further comprising:
determining when transmission of said data element from said first computer system to said second computer system failed; and
repairing said data element without retransmission of said data.
13. (Original) The method of Claim 10, further comprising:
determining when transmission of said data element from said second computer system to said third computer system failed; and
repairing said data element without retransmission of said data.
14. (Original) The method of Claim 11, further comprising:
determining when transmission of said data element from said first computer system to said second computer system failed; and
repairing said data element without retransmission of said data.
15. (Original) An article of manufacture comprising a program storage medium readable by a computer and embodying one or more instructions executable by the computer for causing a computer system to encrypt a data element and decrypt said data element using a static key and a dynamic key, comprising:
encrypting said data element with said static key;
encrypting said data element with said dynamic key; and
decrypting said data element with said static key and said dynamic key.
16. (Original) The article of manufacture of Claim 15 further comprising strongly encrypting said data element with said static key.
17. (Original) The article of manufacture of Claim 15 further comprising weakly encrypting said data element with said dynamic key.

Application No.: 09/872,077

IBM Docket #: STL920000116US1

18. (Original) The article of manufacture of Claim 15, further comprising:
encrypting said data element with said static key on a first computer system;
transmitting said data element to a second computer system;
encrypting said data element with said dynamic key on said second computer system;
transmitting said data element to a third computer system;
decrypting said data element with said static key and said dynamic key on said third computer system; and
thereby distributing encryption between said first computer system, said second computer system, and said third computer system.
19. (Original) The article of manufacture of Claim 15, further comprising:
encrypting said data element with said static key on a first computer system;
encrypting said data element with said dynamic key on said first computer system;
transmitting said data element to a second computer system;
decrypting said data element with said static key and said dynamic key on said second computer system; and
thereby distributing encryption between said first computer system and said second computer system.
20. (Original) The article of manufacture of Claim 18, further comprising:
determining when transmission of said data element from said first computer system to said second computer system failed; and
repairing said data element without retransmission of said data.
21. (Original) The article of manufacture of Claim 18, further comprising:
determining when transmission of said data element from said second computer system to said third computer system failed; and
repairing said data element without retransmission of said data.
22. (Original) The article of manufacture of Claim 19, further comprising:
determining when transmission of said data element from said first computer system to said second computer system failed; and

Application No.: 09/872,077
IBM Docket #: STL920000116US1

repairing said data element without retransmission of said data.

23. (new) A computer system for encrypting and decrypting a data element using a static key and a dynamic key, said data element being partitioned into a plurality of chunks, comprising:
said data element chunks being statically encrypted with said static key;
said data element chunks being dynamically encrypted with said dynamic key; and
said data element chunks being decrypted with said dynamic key and said static key.
24. (new) The computer system of Claim 23 wherein encryption with said static key is strong encryption.
25. (new) The computer system of Claim 23, wherein encryption with said dynamic key is weak encryption.
26. (new) The computer system of Claim 23, wherein:
said data element chunks are encrypted with said static key on a first computer system;
said data element chunks are encrypted with said dynamic key on a second computer system;
said data element chunks are decrypted with said static key and said dynamic key on a third computer system; and
thereby encryption and decryption are distributed between said first computer system, said second computer system, and said third computer system.
27. (new) The computer system of Claim 26, wherein said second computer system is untrusted.
28. (new) The computer system of Claim 23, wherein:
said data element chunks are encrypted with said static key on a first computer system;
said data element chunks are encrypted with said dynamic key on said first computer system;
said data element chunks are decrypted with said static key and said dynamic key on a second computer system; and
thereby encryption and decryption are distributed between said first computer system and said second computer system.

Application No.: 09/872,077

IBM Docket #: STL920000116US1

29. (new) A computer implemented method for encrypting a data element and decrypting said data element using a static key and a dynamic key, said data element being partitioned into chunks, comprising:
- encrypting said data element chunks with said static key;
 - encrypting said data element chunks with said dynamic key; and
 - decrypting said data element chunks with said static key and said dynamic key.
30. (new) The method of Claim 29 further comprising strongly encrypting said data element chunks with said static key.
31. (new) The method of Claim 29 further comprising weakly encrypting said data element chunks with said dynamic key.
32. (new) The method of Claim 29, further comprising:
- encrypting said data element chunks with said static key on a first computer system;
 - transmitting said data element chunks to a second computer system;
 - encrypting said data element chunks with said dynamic key on said second computer system;
 - transmitting said data element chunks to a third computer system;
 - decrypting said data element chunks with said static key and said dynamic key on said third computer system; and
- thereby distributing encryption between said first computer system, said second computer system, and said third computer system.
33. (new) The method of Claim 29, further comprising:
- encrypting said data element chunks with said static key on a first computer system;
 - encrypting said data element chunks with said dynamic key on said first computer system;
 - transmitting said data element chunks to a second computer system;
 - decrypting said data element chunks with said static key and said dynamic key on said second computer system; and
- thereby distributing encryption between said first computer system and said second computer system.

Application No.: 09/872,077

IBM Docket #: STL920000116US1

34. (new) The method of Claim 32, further comprising:
determining when transmission of said data element chunks from said first computer system to
said second computer system failed; and
repairing said data element chunks without retransmission of said data.
35. (new) The method of Claim 32, further comprising:
determining when transmission of said data element chunks from said second computer system
to said third computer system failed; and
repairing said data element chunks without retransmission of said data.
36. (new) The method of Claim 33, further comprising:
determining when transmission of said data element chunks from said first computer system to
said second computer system failed; and
repairing said data element chunks without retransmission of said data.
37. (new) An article of manufacture comprising a program storage medium readable by a
computer and embodying one or more instructions executable by the computer for causing a
computer system to encrypt a data element and decrypt said data element using a static key
and a dynamic key, said data element being partitioned into chunks, comprising:
encrypting said data element chunks with said static key;
encrypting said data element chunks with said dynamic key; and
decrypting said data element chunks with said static key and said dynamic key.
38. (new) The article of manufacture of Claim 37 further comprising strongly encrypting said
data element chunks with said static key.
39. (new) The article of manufacture of Claim 37 further comprising weakly encrypting said
data element chunks with said dynamic key.
40. (new) The article of manufacture of Claim 37, further comprising:
encrypting said data element chunks with said static key on a first computer system;
transmitting said data element chunks to a second computer system;

Application No.: 09/872,077

IBM Docket #: STL920000116US1

encrypting said data element chunks with said dynamic key on said second computer system;
transmitting said data element chunks to a third computer system;
decrypting said data element chunks with said static key and said dynamic key on said third
computer system; and
thereby distributing encryption between said first computer system, said second computer
system, and said third computer system.

41. (new) The article of manufacture of Claim 37, further comprising:
encrypting said data element chunks with said static key on a first computer system;
encrypting said data element chunks with said dynamic key on said first computer system;
transmitting said data element chunks to a second computer system;
decrypting said data element chunks with said static key and said dynamic key on said second
computer system; and
thereby distributing encryption between said first computer system and said second computer
system.

42. (new) The article of manufacture of Claim 40, further comprising:
determining when transmission of said data element chunks from said first computer system to
said second computer system failed; and
repairing said data element chunks without retransmission of said data.

43. (new) The article of manufacture of Claim 40, further comprising:
determining when transmission of said data element chunks from said second computer system
to said third computer system failed; and
repairing said data element chunks without retransmission of said data.

44. (new) The article of manufacture of Claim 41, further comprising:
determining when transmission of said data element chunks from said first computer system to
said second computer system failed; and
repairing said data element chunks without retransmission of said data.